



Reliable and Secure Group Communication

PI: Deb Agarwal

Karlo Berket, Olivier Chevassut,
Guillaume Egles, and Quang Dinh

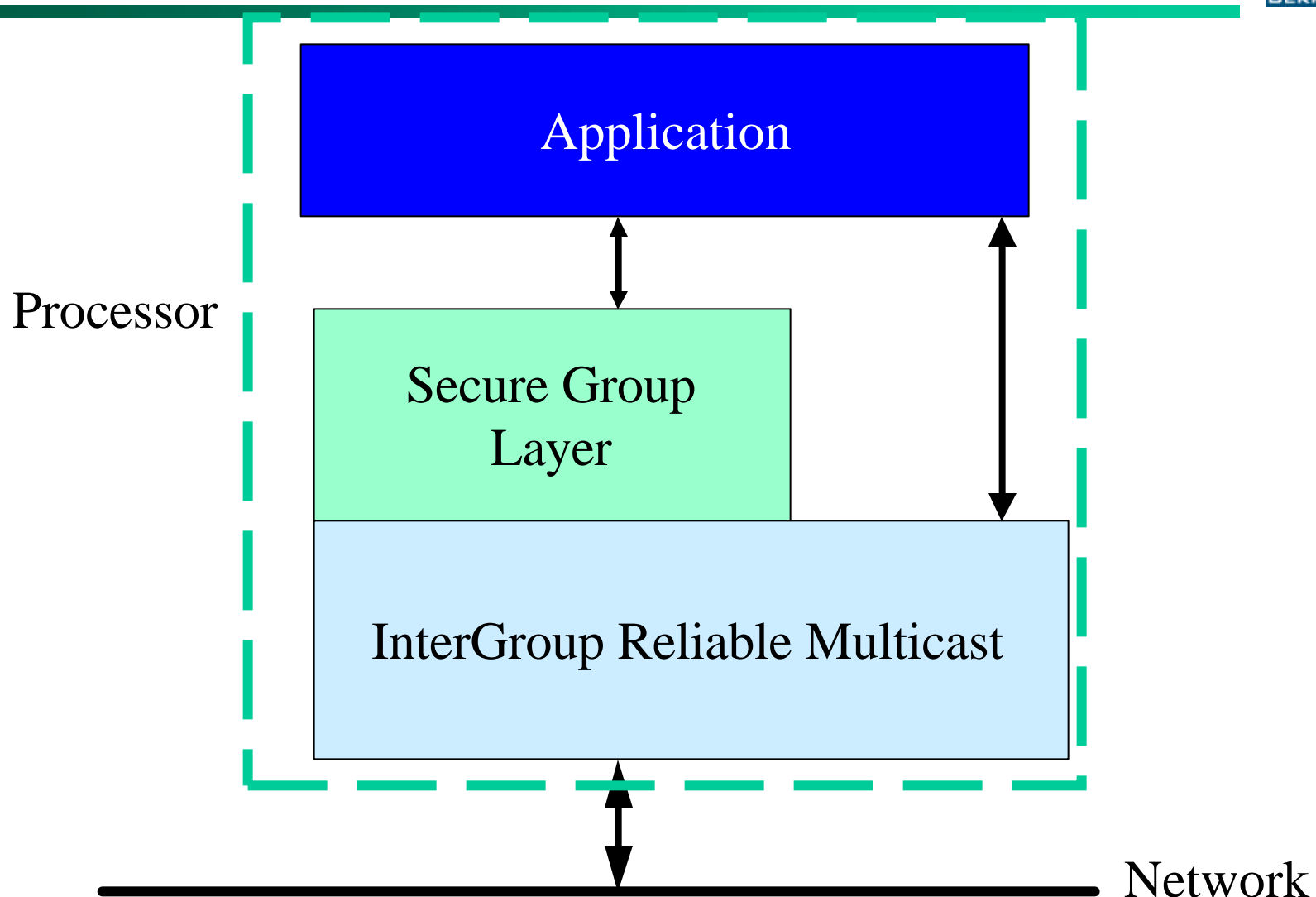
Distributed Systems Department
Lawrence Berkeley National Laboratory

Peer-to-Peer Model



- Allow ad-hoc collaboration
- Remove centralized servers
 - scalable to large collaborations
 - remove bottleneck
- Better model for many collaborations – no central authority
- Easy to add new resources to the collaboration
 - minimize setup required
 - allows local control over resource authorization

System Design

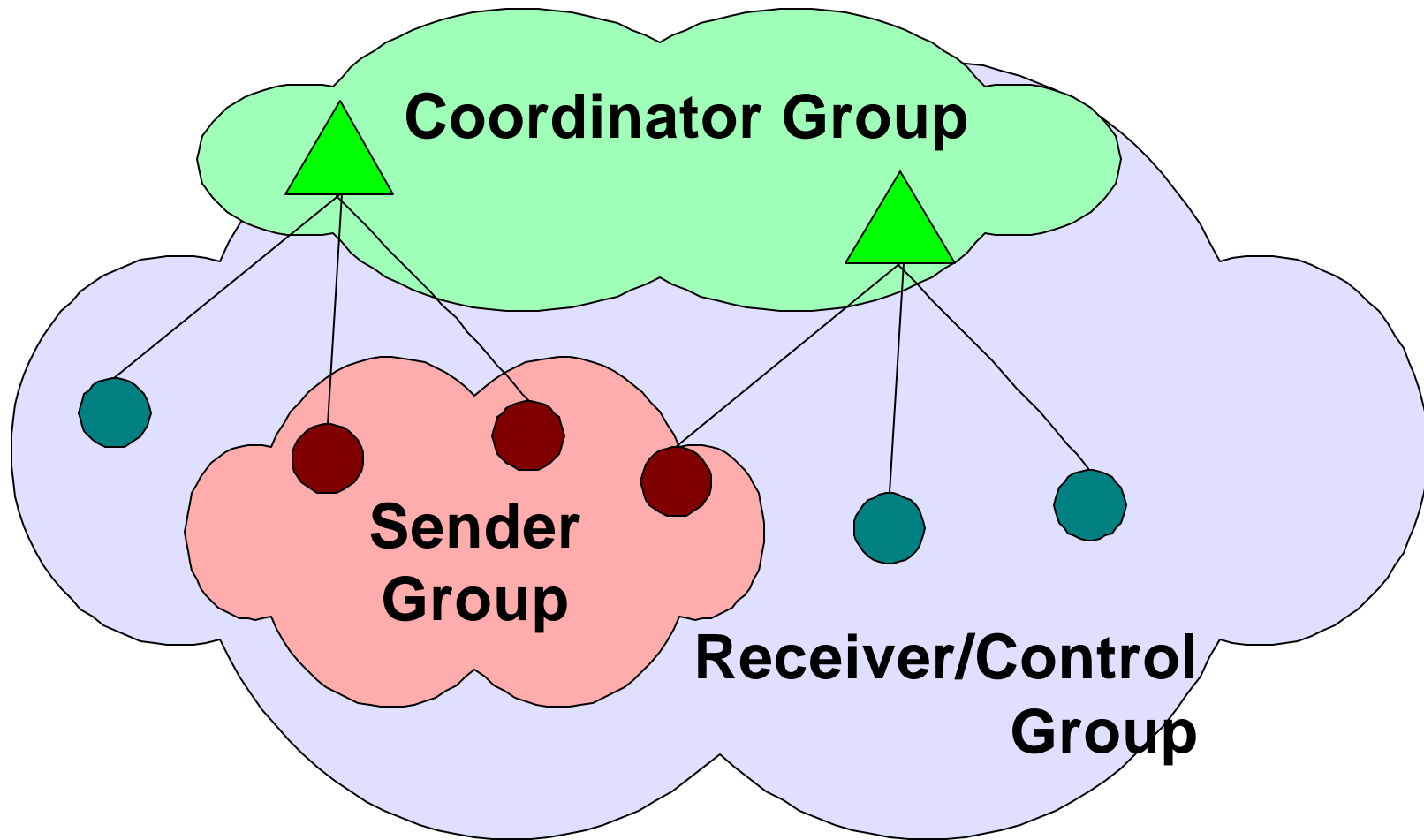


InterGroup Reliable Multicast



- Membership divided into senders and receivers
- Receiver oriented selection of delivery service
 - FIFO order, causal order, or timestamp order
 - Membership changes delivered in order
- Control hierarchy
 - Scalable collection of status information
 - Maintain coordination with receivers

InterGroup Schematic

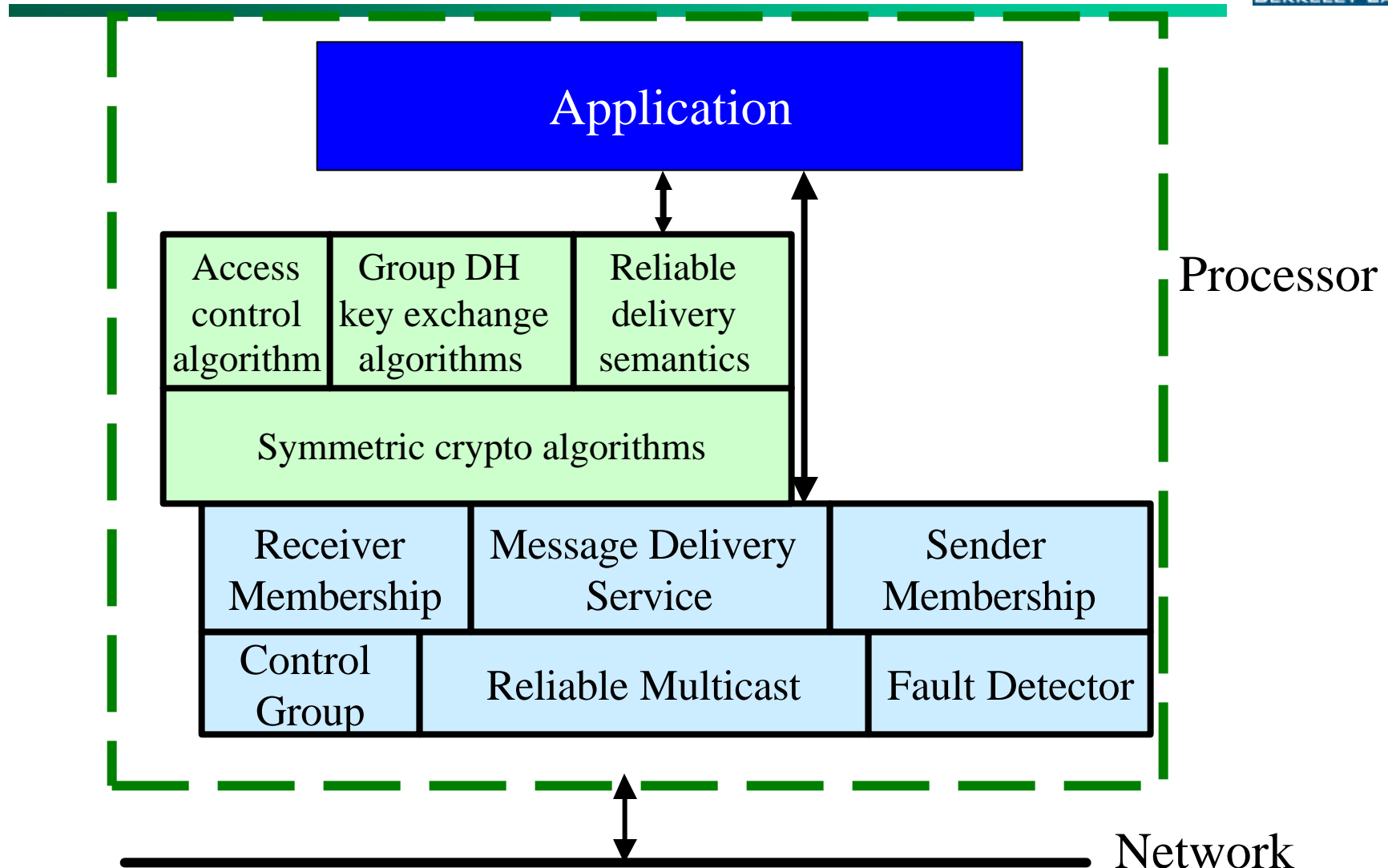


Secure Group Layer (SGL)



- Support dynamic membership
 - members join and leave the group at any time (e.g., network partitions and merges)
 - membership is not known in advance
- Achieve strong security goals
 - authenticated key exchange (AKE)
 - mutual authentication (MA)
 - forward secrecy (FS)
- Provide an SSL-like secure channel

System Design



For More Information



- Self-Configuring Network Monitor
 - Deb Agarwal (DAAgarwal@lbl.gov)
 - Brian Tierney (BLTierney@lbl.gov)
 - www-itg.lbl.gov/Net-Mon/Self-Config.html
- Reliable and Secure Group Communication
 - Deb Agarwal (DAAgarwal@lbl.gov)
 - <http://www-itg.lbl.gov/CIF/GroupComm/>